DoD Public Key Infrastructure (PKI) Update

Rebecca Harris
17 May 2001
(703) 681-0271
harris1b@ncr.disa.mil

Agenda

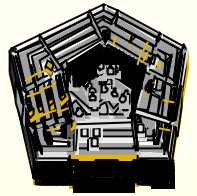
- Introduction – Framing the Problem
- Definition, Concepts, and Components
- DoD PKI
- Interoperability with Trading Partners
- Importance of Applications
- Using the DoD PKI – An Example
- Way Ahead
- Summary

Framing the Problem

- **Deny Participation in a Transaction**

Insider, Hacker, Saboteur, Foreign Intelligence, Enemy CNA, etc...

Commander-in-Chief



Joint Staff

Joint Task Force Commander

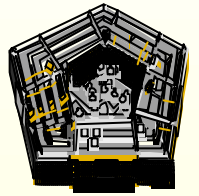
Battlefield Commanders

- **Impersonate Sender**
- **Modify or Delete Data**
- **Read sensitive Data**
- **Gain Unauthorized Access to Networks & Web Servers**

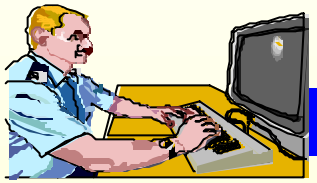
What Does PKI Give Us?

NIPRNet, SIPRNet, Coalition/C2 Networks

Commander-in-Chief



Joint Staff



Joint
Task Force
Commander

Battlefield
Commanders

- ✓ **Authentication of Sender**
- ✓ **Data Integrity**
- ✓ **Data Confidentiality/Recipient Authentication**
- ✓ **Non-repudiation of Transmission/Transaction**
- ✓ **Access Control to Networks & Web Servers**

Definition

- **Public Key Infrastructure (PKI) is:**
  - **Personnel, Policy, Procedures, Components and Facilities to enable cryptographic functions**
- **Key functions include:**
  - **binding User Names to electronic keys,**
  - **publicizing that binding, and**
  - **tracking continued validity of the keys**

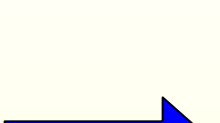
so that applications can provide the desired security services

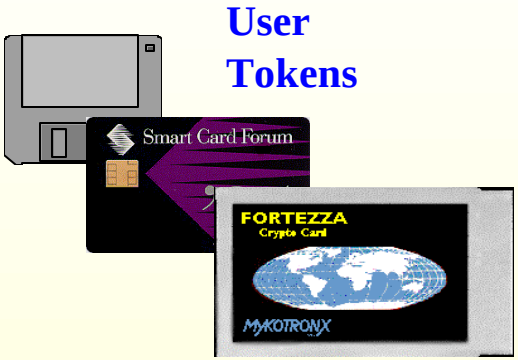
PKI Concepts

MATCHING PUBLIC/PRIVATE KEY PAIRS:

Public

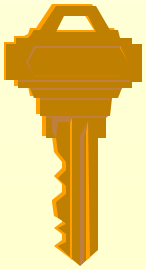
Private



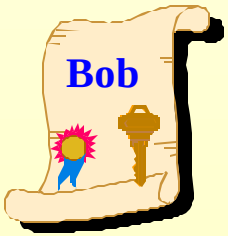


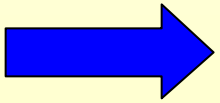
User Tokens

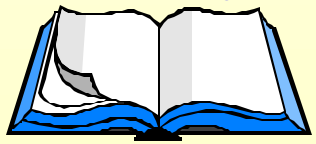
PUBLIC KEY + NAME = CERTIFICATE



Public







Electronic Directory

PKI Key Pairs

Key pairs generated at the same time

Private Key

- Protected by owner
- Used to sign messages
- Used to decrypt messages
- Kept in physical possession of owner

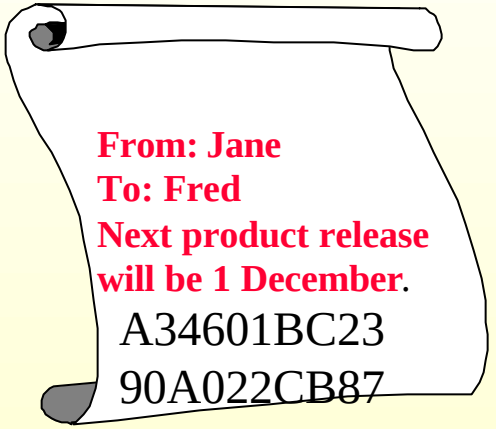
Public Key

- Distributed freely and openly
- Used to verify signatures
- Used to encrypt messages
- Kept in individual public key “certificates”

What is a Digital Signature?

DOCUMENT + **PRIVATE KEY** = **SIGNED DOCUMENT**

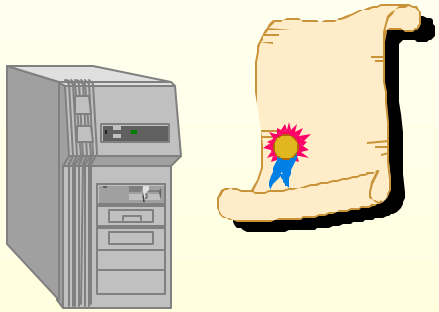
100101100



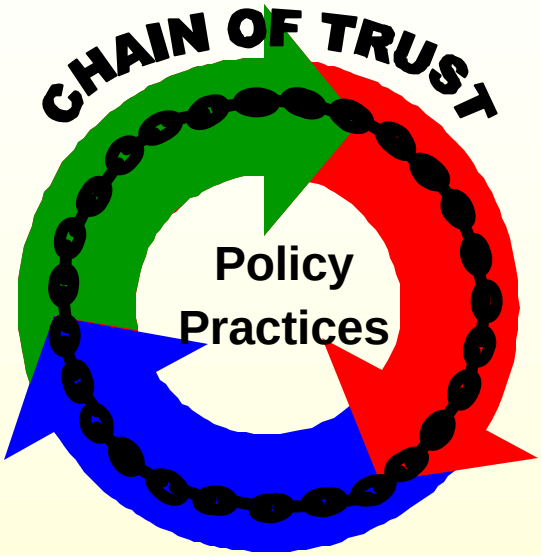
A digital signature is superior to a wet signature because the document can't be changed without detection.

PKI Components

CERTIFICATE MANAGEMENT



- Assert policy
- Certificates
- Interface, processes, procedures, documentation, training
- DISA / NSA



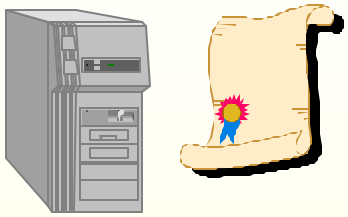
REGISTRATION PROCESS

- Backbone of trust
- Enforce policy
- Acknowledge responsibility
- C/S/As

PK-ENABLED APPLICATIONS

- Application Security
- Relying on Certs and Keys
- C/S/As

PKI Generic Components/Roles



Certification Authority (CA):
creates and signs certificates

Local Registration Authority (LRA):
authorizes creation of certificate
and provides information to CA

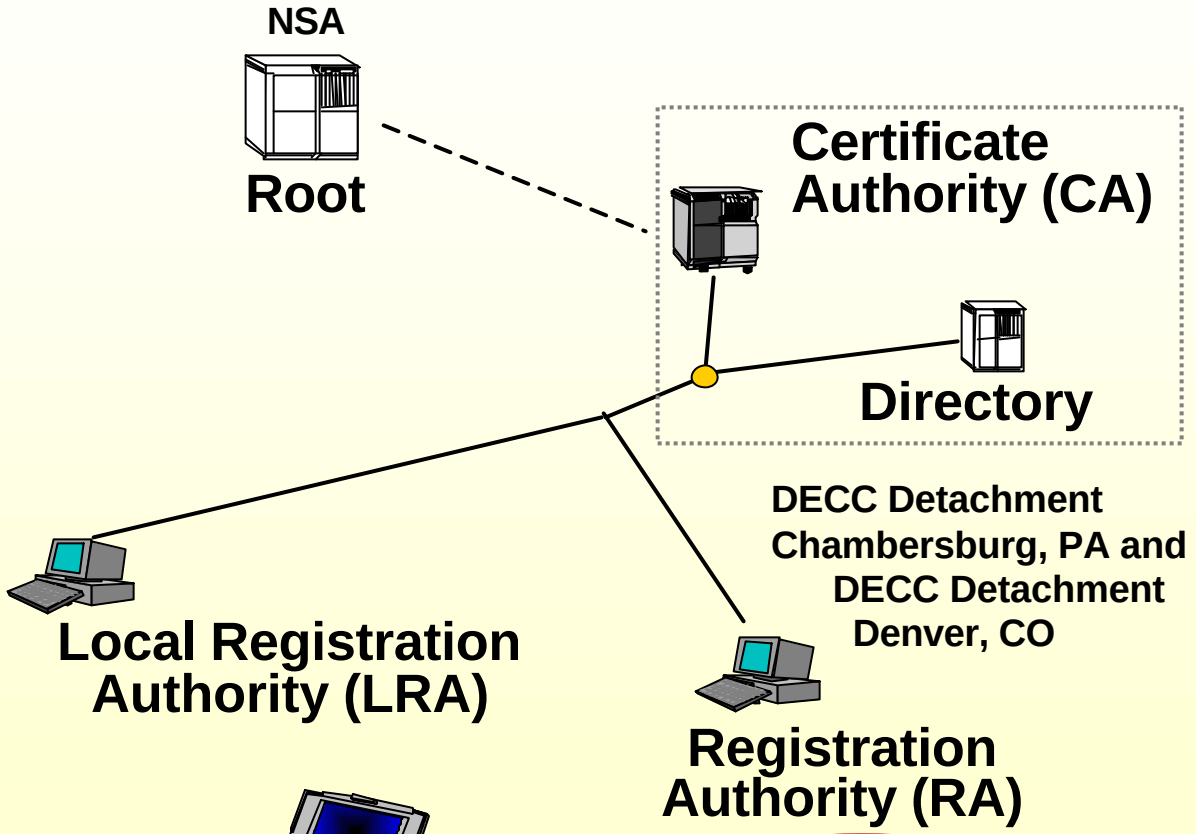
User: requests certificates and uses keys in applications

Relying party: application and/or user who trusts the certificate

DoD PKI Components and Statistics

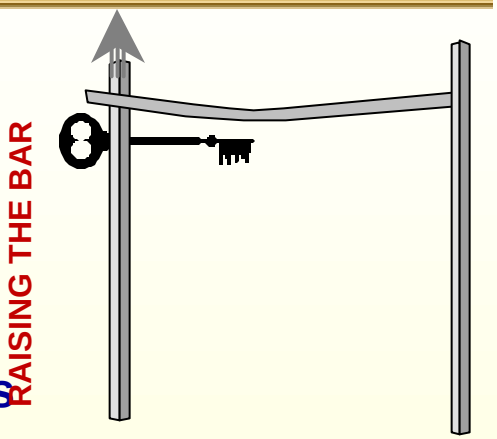
- **Operational on**
  - **NIPRNet**
    - 71,636 identity
    - 54,027 e-mail
    - 7,170 servers
    - 174 RAs
    - 501 LRAs
  - **SIPRNet**
    - 331 identity
    - 26 e-mail
    - 97 servers
    - 13 RAs
    - 13 LRAs

- CA Architecture is highly centralized
- LRAs highly decentralized



24 X 7 Help Desk
1-800-582-4764
weblog@chamb.disa.mil

DoD PKI Release 2.0



- Operational July 31, 2000
- Asserts Class 3 level of assurance
- Enhancements
  - Key Escrow/Key Recovery
  - FIPS 140-1 level 3 hardware signing of certificates
  - Added Policy Object Identifiers to differentiate between HW/SW certificates
  - FIPS 140-1 level 2 smart cards for registration personnel
  - Larger capacity infrastructure
  - Improved firewall protection of the enclaves
- Training
  - RA/LRA Release 2.0 training started in May 00
- DoD PKI RA/LRA Workstation Security Settings Document @ https://iase.disa.mil/documentlib.html#PKIDOCS

DoD PKI Release 3.0 Enhancements and Schedule

- Establishes connection to Defense Enrollment Eligibility Reporting System (DEERS), DEERS provides the PKI Unique Identifier (UID) - the EDI_PI
- Enables Real-time Automated Personnel Identification System (RAPIDS) Verification Officers (VOs) to issue PKI certificates on Common Access Card (CAC)
- Directory Server, Certificate server, and Web Server Software Upgrades
- Schedule:
  - CAC beta — Currently underway
  - System Security Assessment — Currently Underway
  - Release 3.0 NIPRNet — 3rd/4th QTR FY01
  - Release 3.0 SIPRNet — TBD – (After R3 on NIPRNet)

Interoperability with Trading Partners

- **An External Certification Authority (ECA) is an entity authorized to issue certificates that are interoperable with the DoD PKI to non-DoD personnel.**
- **What is an Interim ECA (IECA)?**
  - **Entity authorized to issue certificates interoperable with the DoD PKI to non-DoD personnel, for a period of one year.**
- **Why an *Interim* ECA?**
  - **Need to work out best practices, understand technical and process issues, understand and resolve legal concerns before finalizing ECA approach and processes.**

Common Uses DoD PKI and IECA Certificates

- **Access PKI-enabled web sites**
- **Exchange signed and/or encrypted e-mail**
- **Access and use other PKI-enabled applications**

IECA Status

- **IECA Pilot extended through Sep 01**

Interim External Certificate Authorities:
Digital Signature Trust (DST)
General Dynamics (GD)
Operational Research Consultants (ORC)
VeriSign, Inc.

- **Programs/organizations utilizing IECA certificates**
  - **Medium Grade Services (MGS)**
  - **Joint Electronic Commerce Program Office (JECPO)**
  - **Defense Technical Information Center (DTIC)**
  - **Military Traffic Management Command (MTMC)**
- **Currently testing IECA Server Certificates**
- **Planning to transition IECAs to meet Release 3.0 requirements**

Importance of Applications

- **PKI Certificates Are Only the Enabler**
  - PK Enabled Applications are a Critical Component
- **PKI PMO Primary Responsibilities**
  - Standards-based PKI
  - Design Requirements for PK Enabling Toolkits/Middleware
  - Coordination of Applications Enabling Toolkit/Middleware validation
  - Interoperability Test Capability
- **Organization/Application Responsibilities**
  - Funding
  - Enable Applications
  - Registration Infrastructure

Using the DoD PKI
An Example

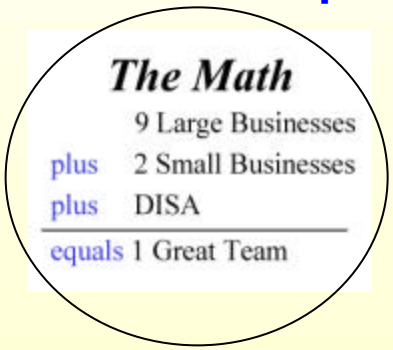
The *I Assure* Advantage

Key Points:

- **Contract supports up to TS / SCI security requirements**
- **7 year multi-award contract**
- **All tasks MUST BE competed, no follow-on work from previous contracts**

Most of the work awarded under this contract will be professional services, however,

…. ***the contract is structured to permit purchase of a full range of Information Assurance (IA) solutions, including the hardware, software and enabling products necessary to implement these solutions.***

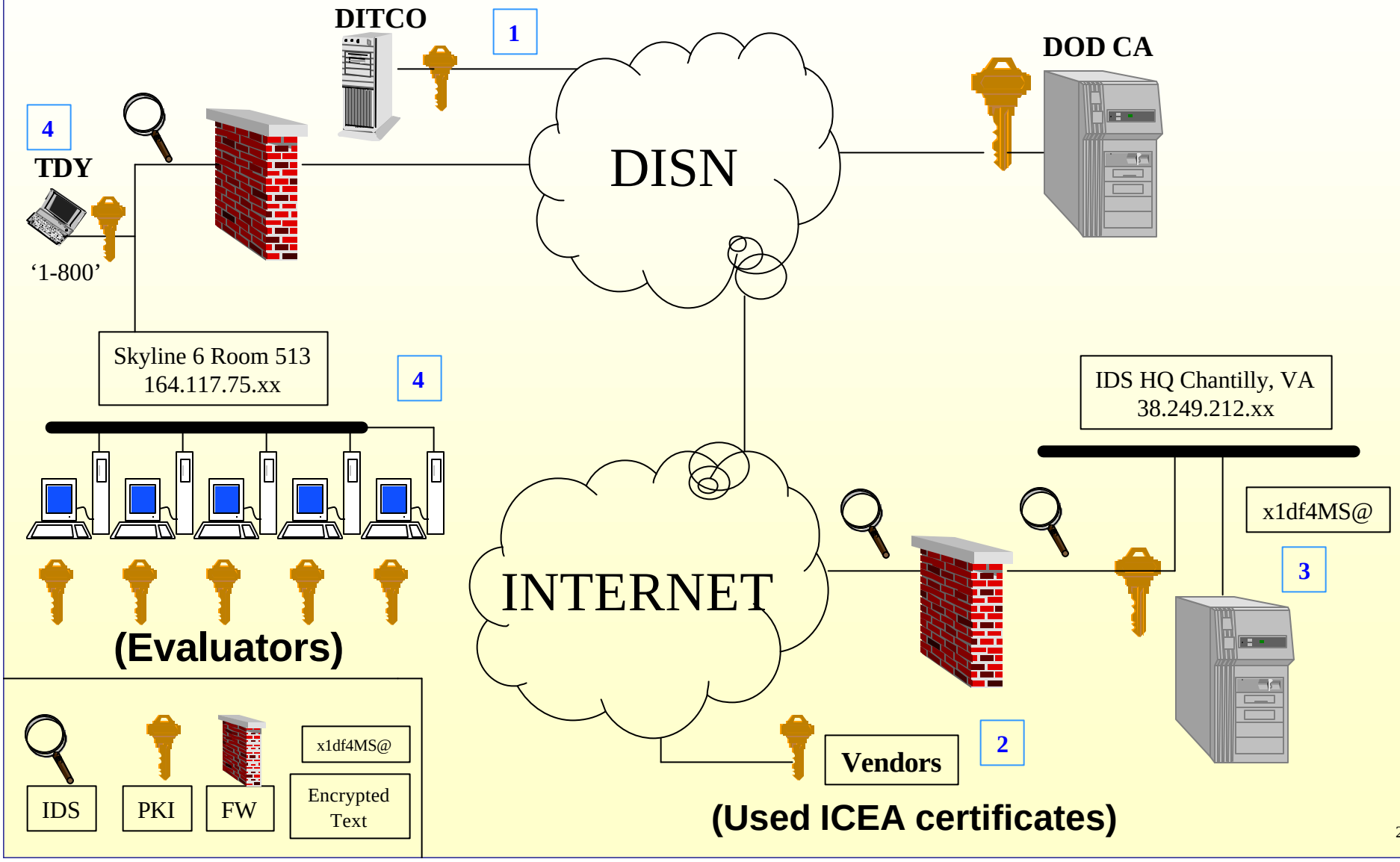


Solutions-based: Contractors can tailor services and products for each task order proposal; Complements Enterprise Software Initiative: I Assure vendors can provide integration services for ESI products

Task Areas:

- **Policy, planning, process, program and project management support**
- **Standards, Architecture, Engineering and Integration support**
- **Solution Fielding / Implementation and operations**
- **Education, training, and awareness; certification and accreditation; and IA support**

DISA 'I ASSURE' - Employed the DoD PKI in the Paperless "Pre-Award" of Contract Process



The Way Ahead

Provide support to Release 3.0

Incremental releases to improve product and service

Expand use of PKI on the SIPRNET

Seamless Transition

Continue Satisfying The Warfighter Requirements!

In Summary

- Establish Trust in Cyberspace
- Provide Secure End-to-End Environment
  - Within DOD, With Commercial Sector, With Allies
- Protect Sensitive But Unclassified
- Create Communities of Interest
- Provide Essential Information Assurance Services


DEFENSE INFORMATION SYSTEMS AGENCY